Document Control No. ECPN SMG.1 10/17/96

Draft

Security Manager's Guide

(SMG)

for the ECPN System

Version 1.0.6.2

10/17/96

Prepared for:

Defense Information Systems Agency (DISA)
45335 Vintage Park Plaza
Sterling, VA 20166-6701

Prepared by:

Inter-National Research Institute, Inc.
12350 Jefferson Avenue, Suite 380
Newport News, Virginia 23602

Authenticated by _____ Approved by _____
(Contracting Agency) (Contractor)

Date _____ Date _____

The following trademarks and registered trademarks are mentioned in this document. Within the text of this document, the appropriate symbol for a trademark (™) or a registered trademark (®) appears after the first occurrence of each item.

HP is a trademark of Hewlett-Packard Company.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

Free Software Foundation, Inc.

Table of Contents

List of Figures

Section 1
Introduction

The Electronic Commerce Processing Node (ECPN) is a Computer Software Configuration Item (CSCI) of the system identified as Electronic Commerce/Electronic Data Interchange (EC/EDI). This guide provides information about ECPN security administration. The Security Manager, or a user assigned a Security Administration role, performs basic tasks such as maintaining audit logs and user accounts.

The following menus appear on the menu bar for the security application:

System Menu
Provides options to set the menu font size for the security application and to exit the system. (Section 2)

Security Menu
Provides options to update audit status, review audit information and archive audit logs. (Section 3)

Accounts Menu
Provides options to create, edit, review, archive, restore, and export roles and user accounts. (Section 4)

Also provided in the Security Manager's Guide, but not listed as a menu option on the menu bar, are printing instructions.

Printing
Provides instructions on printing from an ECPN workstation.

Section 2
System Menu

The System menu provides the following options:

Set Menu Font
To set the font size for menus within the security application. (Section 2.1)

System Exit
To exit the security application. (Section 2.2)

2.1 Set Menu Font

Use the Set Menu Font option to set the font size for the menus within the security application.

From the System menu, select Set Menu Font. The SET MENU FONT window appears.

Figure 2.1-1 SET MENU FONT Window

1. Select the Small, Medium, or Large diamond knob.
2. To accept the change and close the window, click APPLY.
3. Select System Exit from the System menu and restart the security application for the change to take effect.

2.2 System Exit

Use System Exit option to close all windows, exit the security application, and return to the login prompt.

Section 3
Security

The options on the Security menu enable you to maintain and view the audit and alert logs on the workstation. You must log into each workstation operating on the LAN to set its audit status.

The Security menu provides the following options:

Audit Status
To set the level of information allowed on a workstation and to view current logs to determine if they should be archived or purged. (Section 3.1)

Audit Log
To list audit events that occurred since the log was last purged. (Section 3.2)

OS Audit Log
To list events generated by the operating system since the log was last purged. (Section 3.3)

Security Alert Log
To list events generated by the security application since the log was last purged. (Section 3.4)

Archive Logs
To archive alert, audit and OS logs to tape. (Section 3.5)

3.1 Audit Status

The Audit Status option enables you to toggle Security, Auditing, or both, on or off. It also allows you to set the level of granularity for information that should be logged on the workstation and to view the current log sizes to determine when logs should be archived or purged.

From the Security menu, select Audit Status. The AUDIT STATUS window appears.

Figure 3.1-1 AUDIT STATUS Window

The AUDIT STATUS window contains the following features:

1. In the ON / OFF box, toggle the Security and Auditing fields on or off. Security is automatically toggled on, when Auditing is toggled on. Security can be toggled on without Auditing being toggled on.

   Each application running on the workstation determines which events from that application will be logged. When an event is assigned both an audit command and an alert command:

   - The event will be written in both logs if Security and Auditing are toggled on.
   - The event will be written *only* in the SECURITY ALERT LOG if Security is toggled on and Auditing is toggled off.

2. In the GRANULARITY box, select the level of granularity by clicking the appropriate diamond knob. The following granularity levels form a hierarchy; CRITICAL auditing provides the least amount of information, while AMPLIFYING provides the most.

   CRITICAL Events
   : Logging in and out; updating, exporting, or archiving user accounts or roles; archiving and purging logs; changing the audit status; and changing the security classification.

   IMPORTANT Events
   : All CRITICAL events plus user entry or exit of classified functions.

   SIGNIFICANT Events
   : All IMPORTANT events (and, therefore, all CRITICAL events) plus printing or archiving data.

   AMPLIFYING Event
   : All of the above plus all information applications installed on the workstation are designed to collect, such as modifying data in window fields.

3. The LOG SIZES box indicates the size of each log in number of lines (each line representing one event) and in kilobytes. Log sizes are updated as audit records are added. Use the information in this box to determine when logs should be archived and purged.

4. Click APPLY to accept the changes or CANCEL to discard them. Clicking either button closes the window.

3.2 Audit Log

Each workstation operating on the LAN generates an audit log. Each log lists audit events generated by applications running on that machine. Events listed have occurred since the log was last purged. Events will be logged only if Security and Auditing are toggled on in the AUDIT STATUS window.

Because applications determine which events are logged, a comprehensive list of entries for this window is not possible.

From the Security menu, select Audit Log. The SECURITY AUDIT LOG window appears.

Figure 3.2-1 SECURITY AUDIT LOG Window

The SECURITY AUDIT LOG window displays an entry under the following column headings for each audit entry in the log. Click on a column heading to sort the list by that heading. The default sort is the date-time group, listing the most recent record first.

DTG
Date-time group when the audit event occurred.

W/S
The name of the workstation where the audit event occurred.

USER
User at the time of the audit event.

GRAN LEVEL
Granularity of the audit event. (Described in *Audit Status*.)

APP
Application that generated the audit event.

AUDIT EVENT
Description of the audit event.

To print a log:

In the SECURITY AUDIT LOG window, click PRINT to generate a printed report of the window contents. A detailed description of setting up a printer is available in Section 5.

To archive a audit information to tape:

1. In the SECURITY AUDIT LOG window, click ARCHIVE. The ARCHIVE LOG window appears.

2. For instructions on using the ARCHIVE LOG window, see Section 3.5.

To purge audit information from the log:

1. In the SECURITY AUDIT LOG window, click PURGE.

2. A confirmation window appears asking if you want to archive before purging. Archiving a log before purging is strongly recommended.

3. If you select YES in the confirmation window, the ARCHIVE LOG window appears. For instructions on using the ARCHIVE LOG window, see Section 3.5.

4. If you select NO in the confirmation window, another confirmation window appears asking if you are sure you want to purge the log. Select YES to purge or NO to stop the purge.

3.3 OS Audit Log

Each workstation operating on the LAN generates an Operating System (OS) Log. This log lists events generated by the operating system on that machine. Events listed have occurred since the log was last purged.

From the Security menu, select OS Audit Log. The OPERATING SYSTEM LOG window appears.

Figure 3.3-1 OPERATING SYSTEM LOG Window

The OPERATING SYSTEM LOG window displays an entry under the following column headings for each operating system in the log. Click on a column heading to sort the list by that heading. The default sort is the date-time group, listing the most recent record first.

DTG
Date-time group when the OS event occurred.

W/S
The name of the workstation where the OS event occurred.

OS EVENT
Description of the OS event.

To print a log:

In the OPERATING SYSTEM LOG window, click PRINT to generate a printed report of the window contents. A detailed description of setting up a printer is available in Section 5.

To archive a audit information to tape:

1. In the OPERATING SYSTEM LOG window, click ARCHIVE. The ARCHIVE LOG window appears.

2. For instructions on using the ARCHIVE LOG window, see Section 3.5.

To purge audit information from the log:

1. In the OPERATING SYSTEM LOG window, click PURGE.

2. A confirmation window appears asking if you want to archive before purging. Archiving a log before purging is strongly recommended.

3. If you select YES in the confirmation window, the ARCHIVE LOG window appears. For instructions on using the ARCHIVE LOG window, see Section 3.5.

4. If you select NO in the confirmation window, another confirmation window appears asking if you are sure you want to purge the log. Select YES to purge or NO to stop the purge.

3.4 Security Alert Log

Each workstation operating on the LAN generates a security alerts log. This log lists events that should be seen by the Security Manager, generated by security applications running on that machine. Events listed have occurred since the log was last purged.

Events will be logged only if Security is toggled on in the AUDIT STATUS window. Because applications determine which events are logged, a comprehensive list of entries for this window is not possible.

From the Security menu, select Security Alert Log. The SECURITY ALERTS LOG window appears.

Figure 3.4-1 SECURITY ALERTS LOG Window

The SECURITY ALERTS LOG window displays an entry under the following column headings for each alert entry in the log. Click on a column heading to sort the list by that heading. The default sort is the date-time group, listing the most recent record first.

DTG
Date-time group when the audit event occurred.

PRI
Priority of the alert.

W/S
The name of the workstation where the alert event occurred.

USER
User at the time of the alert event.

APP
Application that generated the alert event.

ALERT
Description of the alert.

To print a log:

In the SECURITY ALERTS LOG window, click PRINT to generate a printed report of the window contents. A detailed discription of setting up a printer is available in Section 5.

To archive a audit information to tape:

1. In the SECURITY ALERTS LOG window, click ARCHIVE. The ARCHIVE LOG window appears.

2. For instructions on using the ARCHIVE LOG window, see Section 3.5.

To purge audit information from the log:

1. In the SECURITY ALERTS LOG window, click PURGE.

2. A confirmation window appears asking if you want to archive before purging. Archiving a log before purging is strongly recommended.

3. If you select YES in the confirmation window, the ARCHIVE LOG window appears. For instructions on using the ARCHIVE LOG window, see Section 3.5.

4. If you select NO in the confirmation window, another confirmation window appears asking if you are sure you want to purge the log. Select YES to purge or NO to stop the purge.

3.5 Archive Logs

The Archive Logs option enable you to save the alert, audit, and OS logs to tape.

From the Security menu, select Archive Logs. The ARCHIVE LOGS window appears.

Figure 3.5-1 ARCHIVE LOGS Window

To archive logs:

1. Toggle on any combination of logs to be archived.

2. Insert a tape and click ARCHIVE.

3. Click OK in the confirmation window to verify the archive tape is ready for writing.

4. A second confirmation window appears before proceeding with the archive process. Click YES to continue with the archive, or NO to cancel the process.

   NOTE: The archive process cannot be canceled after YES is selected.

.

This page has been intentionally left blank.

Section 4
Accounts Menu

The Accounts menu provides the following options:

View System Accounts
To view a list of all system accounts provided with the security application. System accounts *cannot* be modified by the Security Manager. (Section 4.1)

View User Accounts
To create, edit, view, and maintain user accounts. (Section 4.2)

View Roles
To create or modify a role. (Section 4.3)

Archive Accts and Roles
To archive accounts and roles to tape. (Section 4.4)

Restore Accts and Roles
To restore accounts and roles to the workstation from tape. (Section 4.5)

Export Accts and Roles
To maintain user accounts and roles on a single workstation and export updated information to multiple workstations on the LAN. (Section 4.6)

4.1 View System Accounts

The View System Accounts option enables you to view a database of all system accounts provided with the security application. System accounts include accounts that are required by the operating system. The list of accounts will vary, depending on the hardware platform running the security application.

Using the View System Accounts option, you can do the following:

- View the system accounts database.
- Generate a printed report.

To view the system accounts database:

From the Accounts menu, select View System Accounts. The SYSTEM ACCOUNTS window appears.

Figure 4.1-1 SYSTEM ACCOUNTS Window

The data in the SYSTEM ACCOUNTS window is provided for information purposes only and cannot be modified. The window provides an entry under the following column headings for each system account in the database:

LOGIN NAME
Login name assigned to the account.

USR ID
Number assigned to the user by the system.

DESCRIPTION
Description of the account.

To generate a printed report:

1. In the SYSTEM ACCOUNTS window, click PRINT. The JMCIS PRINTER window appears.

2. See Section 6 for instructions on using the JMCIS PRINTER window.

4.2 View User Accounts

The View User Accounts option enables you to create, edit, view and maintain user accounts. The accounts include default accounts and accounts added by any user that is assigned a Security Administrator role.

Three default user accounts are provided with the security application:

root - privileged user account for the workstation; allows unrestricted access to all UNIX files.
secman - security administration user account
sysadmin - system administration user account

The default accounts are protected system files. For these accounts, *only* the password can be modified.

Important: The default password for the *root, secman,* and *sysadmin* accounts is *vinson*. It is strongly recommended that the password for these accounts be changed immediately after the first login.

Using the View User Accounts option, you can do the following:

- Access the user accounts database.
- Create a user account.
- Delete a user account.
- Edit a user account.
- Generate a printed report.
- Retain a user account marked for deletion.

To access the user accounts database:

From the Accounts menu, select View User Accounts. The USER ACCOUNTS window appears.

Figure 4.2-1 USER ACCOUNTS Window

The USER ACCOUNTS window lists all accounts in the user account database. The data listed for each account entry is displayed under the following column headings:

*****

A (add), D (delete), or M (modify) indicate pending changes made to the account.

LOGIN NAME

Name used at login.

USER ID

Number assigned to the user by the system.

DESCRIPTION

Description of the account.

To create a user account:

1. Determine if:
   - A default role will be assigned to the account.
   - A role should be created (as described in Section 4.3).

2. In the USER ACCOUNTS window, click ADD. The ADD ACCOUNT window appears.

Figure 4.2-2 ADD ACCOUNT Window

3. In the LOGIN NAME field, enter a login name (3-10 characters) for the account.

4. (Optional) In the DESCRIPTION field, enter a short (up to 35 characters) description of the account.

5. From the ACCOUNT GROUPS box, select one or more account groups for the user account. An account group defines access to applications.

6. From the ROLES box, select one or more roles for the user account. A role assigns a specific functionality within an application. Each user account is assigned one or more of these account groups:

   root - direct access to Unix
   System Admin - access to the system administration applications
   Security Admin - access to the security applications
   JMCIS Operator - access to the operator applications

7. Click OK to accept the new account. The PASSWORD window appears.

8. Enter a password (6-8 characters). Press Return and re-enter the password to confirm it.

9. Click OK to save the new password. The USER ACCOUNTS window reappears, displaying an A in the * column for the account.

10. When you are finished making changes in the USER ACCOUNTS window, click SAVE or OK to accept the new account. If you click CANCEL, all changes made in the USER ACCOUNTS window will be discarded.

To delete a user account: (Default accounts cannot be deleted.)

1. In the USER ACCOUNTS window, select one or more account entries.

2. Click DELETE. A confirmation window appears to verify the delete.

3. Click YES to confirm the delete. The USER ACCOUNTS window reappears, displaying a D in the * column for the account.

4. When you are finished making changes in the USER ACCOUNTS window, click SAVE or OK. If you click CANCEL, all changes made in the USER ACCOUNTS window will be discarded.

To edit a user account:

1. In the USER ACCOUNTS window, select an account entry.

2. Click EDIT. The EDIT ACCOUNT window appears.

Figure 4.2-3 EDIT ACCOUNT Window

3. For instructions on editing an account, see the instructions provided for Figure 4.2-2.

4. To edit the password, click PASSWORD. The # characters in the PASSWORD field must be deleted before a new password can be entered.

   Note: For a default account, only the password can be modified.

5. Click OK to save the account modifications. The USER ACCOUNTS window reappears, displaying an M in the * column for the account.

6. When you are finished making changes in the USER ACCOUNTS window, click SAVE or OK. If you click CANCEL, all changes made in the USER ACCOUNTS window will be discarded.

To generate a printed report:

In the USER ACCOUNTS window, click PRINT. See Section 5 for a detailed description of how to set up a printer.

To retain a user account marked for deletion:

Select UNDELETE from the pop-up menu for the USER ACCOUNTS window. The D in the * column for the entry will disappear, and the account will remain in the list.

4.3 View Roles

The View Roles option enables you to create or modify a role. A role specifies a user's access to menus and options. Use the View User Accounts option to assign a role to a user account.

A role definition includes:

- role name
- security level
- account group
  - -- ECPN Operator, System Admin, or Security Admin
  - -- roles may not be created for root
- access to the menus and options within the account group
- capability permissions

A role is also used to track login and logout events in the audit log. Multiple roles may be created for an account group and multiple account groups and roles may be assigned to a user account. The user's role will appear in the right-hand corner of the ECPN main menu bar.

Three default roles delivered with the system provide access to all functions of the assigned account group:

- SSO Default
  - -- Security Admin account group
  - -- Access to all security application menus and options
  - -- Top Secret classification
- SA Default
  - -- System Admin account group
  - -- Access to all system administration menus and options
  - -- Top Secret classification
- ECPN Default
  - -- ECPN Operator account group
  - -- Access to all ECPN COE segment and ECPN application segment menus and options
  - -- Top Secret classification

Using the View Roles option, you can do the following:

- Access the user roles database.
- Create a user role.
- Delete a user role.
- Edit a user role.
- Duplicate a user role.
- Generate a printed report.

To access the user roles database:

From the Accounts menu, select View Roles. The USER ROLES window appears.

Figure 4.3-1 USER ROLES Window

Each entry in the USER ROLES window includes data under the following column headings:

ROLE
Name of the role.

ACCT GROUP
Account group associated with the role.

CLASSIFICATION
Security classification level of the role.

To create a user role:

1. In the USER ROLES window, click ADD. The ADD ROLE window appears.

Figure 4.3-2 ADD ROLE Window

2. In the NAME field, enter a name for the role, not to exceed 15 characters.

3. Click the SECURITY field, and choose a security level from the list that appears.

4. From the ACCOUNT GROUPS box, select one account group to specify which application will be available to a user assigned to this role.

5. Click OK to accept the new role. The EDIT ROLE window (described below) opens to allow you to define the role.

To delete a role:

Note: Default roles and roles assigned to a user account cannot be deleted.

1. In the USER ROLES window, select one or more roles.

2. Click DELETE. A confirmation window appears to verify the delete.

3. Click YES to confirm the delete. The role is deleted from the USER ROLES list and will not appear in the ROLES list in the ADD ACCOUNT window.

To edit a role:

Notes about editing a role:

- Access to menus and functions can be expanded or reduced.
- When new segments are loaded, additional menus and options will be available. A role can be expanded to include the added functionality.
- When segments are removed, menus and options are automatically deleted from associated roles. However, user accounts assigned the roles will retain the previous role information.
  -- Open the EDIT window for each user account and modify at least one field.
  -- The user account will then incorporate the revised role. (See Section 4.2.)

1. In the USER ROLES window, select a role and then click EDIT. The EDIT ROLE window appears.

Figure 4.3-3 EDIT ROLE Window

2. In the ROLE HEADER box, click the SECURITY field and choose a security level from the list that appears.

3. Use the PERMISSIONS box to define functions available to a user assigned the role.

   Categories and functions that appear in the PERMISSIONS box depend on the account group selected for the role. The account groups with their categories and subset of functions are as follows:

Security Admin

Category	Add	Delete	Edit	Print	Restore	Archive	Export
Accounts							

Audit Status Classification Logs Roles							
	X	X	X	X	X	X	X
			X				
			X				
		X		X		X	
	X	X	X	X	X	X	X

ECPN Operator

Not available at this time.

System Admin

Category	Mount	Unmount	NEWFS	Init Floppy	Mount New	Add	Delete	Edit
DiskManager	X	X	X	X	X			
EditHosts						X	X	X

Root

No roles can be associated with this account group.

a. In the PERMISSIONS box, select one category in the scroll list and then click EDIT. The EDIT PERMISSIONS window appears.

Figure 4.3-4 EDIT PERMISSIONS Window

b. Toggle checkboxes on for functions to be available to a user assigned this role. (All functions are OFF when a new role is created.)

- For example, in Figure 5.3-12, a user could add, print, restore, archive and export, but could not delete or edit.
- The list of functions shown for the selected category is an appropriate subset of the potential functions.

c. Click OK to accept the changes, or CANCEL to discard. Clicking either closes the window.

d. Repeat steps 1.

4. Use the MENU ACCESS box to select the menus and options for the role.

a. The MENU ACCESS box contains a scroll list of the menu bars found in the application accessible to a role. Use EDIT to define which menus and options will be available.

b. Select one menu bar in the scroll list and then click EDIT to open the EDIT MENU ACCESS window. This window contains a list of menus on the menu bar of an application. (Applications are designated by the account group selected for the role.)

c. Click the arrow left of the menu name to reveal a cascading list of options for that menu.

d. Toggle menus and options on or off. (All menus and options are on when a role is created.)

- If a menu or option is on (shaded) it is available to a user assigned this role.
- If a menu or option is off (blank) it will not appear on the menu bar or the pull-down menu for a user assigned this role.

e. Click OK to accept the changes.

f. Repeat this process for other menu bars in the scroll list.

5. In the EDIT ROLE window, click OK to accept the role.

To duplicate a role:

1. From the USER ROLES window, select a role to duplicate.

2. Click DUPLICATE.

3. In the DUPLICATE ROLE window, enter a new role name.

4. Click OK to accept the name and close the window. The duplicate role is listed in the USER ROLES window. Use EDIT to make changes to the new role.

To generate a printed report:

In the USER ROLES window, click PRINT. See Section 5 for a detailed description of how to set up a printer.

4.4 Archive Accts & Roles

The Archive Accts & Roles option enables you to archives user account and role information to tape.

From the Accounts menu, select Archive Accts & Roles. The ARCHIVE ACCTS & ROLES window appears.

Figure 4.4-1 ARCHIVE ACCTS & ROLES Window

To archive accounts and roles:

1. Toggle Accounts or Roles, or both, on.

2. Click ARCHIVE (or, click CANCEL to discontinue the archive process).

3. Insert a tape and click OK in the warning window.

4. A confirmation window appears before proceeding with the archive process.

   - Note: The archive process cannot be canceled after YES is selected.
   - Click YES to continue with the archive, or NO to cancel the process.

4.5 Restore Accounts & Roles

The Restore Accts & Roles option enables you to restores all accounts or roles from tape.

To restore accounts and roles:

1. NOTE: The restore option *overwrites* the current account and role information on the workstation where the tape is loaded.

2. Select the Restore Accts & Roles option from the Accounts Menu.

3. Insert the tape and click OK in the warning window.

4. A confirmation window appears before proceeding with the restore process.

5. Click YES to continue (or NO to cancel the process).

6. The table of contents on the tape is displayed in the RESTORE ACCTS & ROLES window.

Figure 4.5-1 RESTORE ACCTS & ROLES Window

7. Click RESTORE to read the tape and overwrite the account and role information on this workstation (or click CANCEL to retain role and account information).

4.6 Export Accts & Roles

The Export Accts & Roles option enables you to maintain user accounts and roles on a single workstation and export the updated information to multiple workstations on the LAN.

From the Accounts menu, select Export Accts & Roles. The EXPORT LIST window appears.

Figure 4.6-1 EXPORT LIST Window

The window contains a scroll list of workstations on the LAN. Maintain the workstation list to prepare to export accounts and roles:

- Check the status of all workstations.
- Check for duplicate workstation entries.
- Add or delete workstations.

To export information:

1. NOTE: User accounts and roles from the local machine will *overwrite* the user account and role information on the destination machines.

2. Update account and role information on this workstation.

3. Check the status of the destination machines using the STATUS or SCAN buttons.

4. Select the destination machines in the workstation list (or click SELECT ALL).

5. Click EXPORT to send the updated accounts and roles to the selected workstations.

To ping each workstation in the list:

STATUS pings each workstation in the list.

- A workstation which responds is labeled UP in the status column.
- A workstation which does not respond is labeled DOWN.
- Double-click on a workstation in the list to check its status.
- The STATUS function may be run at any time and does not interfere with the network.

DUPS checks for multiple workstation entries with the same network and host identification. When duplicates are found, they are listed in the REMOVE DUPLICATES window.

1. Highlight an entry in the REMOVE DUPLICATES window scroll list.

2. Click SELECT to remove that duplicate workstation name.

3. Click SKIP to retain both workstation names and go to the next duplicate.

4. Click ABORT to close the window.

SCAN searches the network for all available ECPN workstations.

- Displays the total number of workstations added to the list.
- This function can be run at any time and does not interfere with the network.

SELECT ALL highlights all workstations on the list. Select UNSELECT ALL from the window's pop-up menu to unselect all workstations in the list.

EXPORT exports account and role information from the local machine to selected machines.

1. Highlight the destination machines (must be designated as UP).

2. Click EXPORT.

To add a workstation to the list:

1. Click ADD to open the ADD W/S window.

2. Enter the new workstation name.

3. Click OK to add it to the list or click CANCEL to discard the change.

To delete workstations from the list:

1. Highlight the workstations

2. Click DELETE.

Section 5
Printing

Before ECPN operators have access to printers, two steps must be taken:

1. Define the printers available on the network and identify which workstations have access to each printer. This is a System Administrator function that cannot be accessed by ECPN operators.

2. On each workstation, identify the default line, graphic, and Unix printers for that workstation. Use the Printer Chooser option on the Misc pull-down menu.

This procedure must be followed when ECPN applications are loaded and whenever printers are added, relocated, or removed from the network.

To print from an ECPN option:

In many windows, a printed report summarizing the window information can be generated using the PRINT function. Choosing PRINT opens the ECPN PRINTER window to identify where the report will be printed.

When the window appears, the printer listed in the Selected Printer box is the default printer, also shown in the Default Printer box.

- All fields in the Selected Printer box except Copies cannot be edited.
- All fields in the Default Printer box cannot be edited. Another default printer is selected using the Printer Chooser option (MISC pull-down menu).

The fields in the Selected Printer and Default Printer boxes are:

PRINTER
Printer type.

NAME
Printer name.

HOST
Workstation to which the printer is connected.

STATUS
Indicates if the printer is ready or in use.

COPIES
Number of copies to print. To change the value in the Selected Printer box, enter a number. In the Default Printer box this field is view only.

The scroll list displays a list of printers on the LAN available to this workstation. The following columns are displayed for each printer:

PRINTER NAME
Printer type.

HOST
Workstation to which the printer is connected.

REMARKS
Remarks about the printer.

To send the report to the printer:

1. Choose a printer.

   - To use the default printer, no action is required.
   - To choose a different printer, highlight the printer in the scroll list. The fields for this printer appear in the Selected Printer box.

2. Specify the number of Copies in the Selected Printer box.

3. Click OK to send the report to the selected printer.